DOE CIO Guidance CS-14

U.S. Department of Energy

Cyber Security Program

PORTABLE/MOBILE DEVICES GUIDANCE

January 2007

This Guidance document was developed and issued outside of the Departmental Directives Program.

1. PURPOSE.

   This Department of Energy (DOE) Chief Information Officer (CIO) Guidance provides additional direction on the secure use of portable and/or mobile devices within the DOE. In addition, this Guidance establishes processes for the use of portable/mobile devices (e.g., notebook computers, workstations, personal digital assistants,etc.) within and outside of DOE security areas. It reflects the requirements from applicable Public Laws, Federal Regulations, Departmental Directives, and previously issued DOE CIO Guidance and also considers additional controls that may be required resulting from a risk assessment.

   The DOE Office of the Chief Information Officer (OCIO) will review this Guidance annually and update it as necessary. The DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) and their subordinate organizations and contractors (hereinafter called operating units) may provide feedback at any time for incorporation into the next scheduled update.

2. SCOPE.

   This Guidance provides additional information for Senior DOE Management for addressing the controls in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance,* and DOE Manual 205.1-4, *National Security Systems Controls Manual*, in their Program Cyber Security Plans (PCSPs). Specifically, this Guidance applies to computing devices that are considered to be portable/mobile devices.

3. CANCELLATIONS.

   None.

4. APPLICABILITY.

   a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to Which DOE CIO Guidance CS-14 is Applicable.*

      Further, Senior DOE Management may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their operating units, and for ensuring that those requirements are incorporated into contracts.

   b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear

Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.

c. DOE Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all systems hosting unclassified information. DOE CIO Guidance CS-38A, *Protection of Sensitive Unclassified Information, Including Personally Identifiable Information Guidance*; DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*; and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provide additional information for identifying unclassified information requiring protection.

d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security Systems. The protection mechanisms described in this guidance are consistent with and implement the policies and practices set forth by Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPOM);* the Atomic Energy Act of 1954, which established Restricted Data information; and EO 12958, *Classified National Security Information*, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information.. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides additional guidance for identifying National Security systems.

5. IMPLEMENTATION.

This Guidance is effective 30 days after issuance. However, DOE recognizes that this Guidance cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its issuance. If Senior DOE Management cannot address all of the criteria by that date, Senior DOE Management is to establish a Plan of Actions and Milestones for implementation of this Guidance into their PCSP.

6. CRITERIA. .

a. Senior DOE Management PCSPs must define policies, processes, and procedures for the use of portable/mobile devices to include at least the following:

(1) Policies and processes governing the use of Government-owned portable/mobile devices.

(2) Policies and processes governing the use of personally owned portable/mobile devices in close proximity to, e.g., in the same room as, information systems processing Government information (e.g. unclassified information, Sensitive Unclassified Information, or classified information).

b. Program Cyber Security Plan. Senior DOE Management PCSPs are to be consistent with the criteria in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*, and DOE M 205.1-4*, National Security Systems Controls Manual*. To ensure consistency with these controls, Senior DOE Management PCSPs are to direct operating units to develop, document, and implement portable/mobile device policies and procedures consistent with the following criteria and commensurate with the level of security required for the organization's environment and specific needs. Senior DOE Management PCSPs are to require operating units to define and document the following

(1) Policies for the protection and transportation of portable/mobile devices, components of portable computing devices (e.g., removable disk or disk drives, etc.), containing sensitive, classified or unclassified, information

(2) A process for approving where portable/mobile devices will be permitted. Policies should address the use of portable/mobile devices for each security area under the cognizance of the operating unit.

(a) Portable/mobile devices used to process DOE information and taken outside the United States, other than the assigned user's primary work location, must be sealed with Senior DOE Management approved tamper-indicating devices prior to removal of the computing device from the user's primary location. The tamper-indicating devices must be placed to allow normal use (i.e., removal and insertion of components such as removable hard drives and batteries). The cognizant Designated Approving Authority (DAA) may approve alternative protection measures when the use of tamper-indicating devices are ineffective or for operational requirements.

(b) Portable/mobile devices used to process DOE information and taken outside the United States, other than the assigned user's primary work location, must be subjected to a hardware and software technical review process, as defined in the Senior DOE Management PCSP, upon return to detect unauthorized changes.

(c) The operational environment and protections for each portable/mobile device is described in a System Security Plan (SSP). The SSP must identify restrictions and special security considerations for use in different security areas including at home or off-site.

(d) Administrative and physical controls to reduce/ eliminate the DOE TEMPEST/ TSCM concerns when allowing the operation of portable/ mobile devices with a wireless and/or audio or video recording capability in operating unit security areas must be documented in the portable/ mobile system's SSP.

(3) A process for reporting, as an incident, unauthorized information content on and theft, loss, or misplacement of portable/ mobile devices used to process DOE information. Requirements for incident handling and reporting are outlined in DOE CIO Guidance CS-9, *Incident Management*.

(4) Personnel training requirements for the use for portable/ mobile computing devices.

(5) A process to ensure that visitors to any area where DOE sensitive unclassified information or classified is being processed on cyber systems are advised of the requirements for the secure use of portable/ mobile devices

(6) A policy for the use of portable/mobile devices with radio frequency (RF) or Infra-red (IR) capability (e.g. Wireless Information System [W-IS]) in operating unit security areas where Government information is processed, stored, transferred, or accessed on information systems, or where sensitive unclassified or classified information is discussed or displayed via electronic methods. The policy is to include the following:

(a) Authentication of all users in accordance with the devices's approved SSP;

(b) Employment of up-to-date malicious code detection software;

(c) Compliance with applicable National Telecommunications and Information Administration (NTIA) and Federal Communication Commission (FCC) requirements;

(d) Compliance with PCSP requirements;

(e) Configuration with preferences and settings for services approved by the cognizant DAA; and

(f) Configuration managed and controlled.

(7) A process to ensure that personally owned portable/mobile devices:

(a) May be used in or brought into an area where DOE Sensitive Unclassified Information (SUI) is being processed on an information system only in accordance with the policies and procedures defined in the PCSP and documented in the device's associated System Security Plan (SSP).

(b) May connect to DOE or DOE contractor information systems processing DOE information only if allowed by the PCSP and information system's SSP.

(c) Are allowed to process DOE SUI only in accordance with the policies and procedures defined in the PCSP and documented in the device's associated SSP.

7. CRITERIA UNIQUE TO NATIONAL SECURITY SYSTEMS. Senior DOE Management PCSPs are to require operating units to define and document the following:

   a. Policies prohibiting the use of personally owned portable/ mobile devices and media in areas where classified data are discussed or processed.

   b. Policies prohibiting the use of personally owned portable computing devices and media from storing, processing, receiving, or transmitting classified information.

   c. Compliance with TEMPEST (Study of Compromising Emanations) and Protected Transmission System policies for all portable/ mobile devices processing, displaying, storing, or transmitting classified information.

   d. Compliance with DOE Technical Surveillance Countermeasures policies for all portable and mobile devices processing, displaying, storing, or transmitting classified information.

   e. Protected Transmission Systems for all communications to/ from the portable/ mobile devices accredited for processing classified information.

   f. Policies prohibiting portable/ mobile devices accredited for classified processing from:

      (1) Downloading or loading any freeware or shareware enhancements or any extraneous software.

      (2) Synchronizing with any unclassified system.

8. REFERENCES.

   Other references are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls*.

9. DEFINITIONS.

   Acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

   Personally Owned: Information systems, devices, media, or equipment owned by individuals and entities (e.g., businesses, colleges, etc) that are not included in a DOE SSP or controlled under a DOE PCSP. Personally Owned Devices include, but are

not limited to, personal computers and related equipment, handheld and Personal Digital Assistant (PDA) devices, facsimile machines, photocopiers, enhanced cell phones, and storage devices such as flash memory (memory sticks), flash cards, portable hard drives, and MP3 players.

Portable/ Mobile devices: Portable and mobile devices are portable computing devices that provide the capability to collect, create, process, transmit, store, and disseminate information. These devices include (but are not limited to) handheld and Personal Digital Assistant (PDA) devices, facsimile machines, photocopiers, MP3 players, notebook computers, mobile work stations, web enhanced cell phones, two way pagers, and wireless e-mail devices.

10. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO GUIDANCE CS- 14 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Health, Safety, and Security
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration